ARGUMENTS/REMARKS

Applicants would like to thank the examiner for the careful consideration given the present application. The application has been carefully reviewed in light of the Office action, and amended as necessary to more clearly and particularly describe and claim the subject matter which applicants regard as the invention.

Claims 1-35 remain in this application. Claims 36 and 37 have been added.

Claim 25 was rejected under 35 U.S.C. §103(a) as being unpatentable over Gelman *et al.* (U.S. 6,415,329) in view of RFC2246 ("The TLS Protocol, Version 1.0"). For the following reasons, the rejection is respectfully traversed.

Claim 25 recites a method by which a terminal can access a server with the terminal sending a request for the server to a gateway, wherein "security utilized between said terminal and said gateway is based on a *first security protocol*...including an *encryption*" and wherein the server is secured "with a *second security protocol*...also including an *encryption*" (emphasis added). The method includes the step of "*converting* between said first and said second security protocol in a secured domain of said *server*", wherein "*encrypted* packets sent by said terminal are routed by said gateway to said secured domain *without* said gateway decrypting *all* of the packets transmitted during a session" (emphasis added).

In contrast, Gelman does not disclose central features of the claim, because Gelman teaches that there are two gateways (see Figs. 1 and 2) and that there is a conversion on gateway 12 from a *first* protocol, then a transmission over wireless link 22 using a wireless protocol, and then a conversion back to the *first* protocol on gateway 16. Gelman, at col. 2, lines 55–57, clearly states that "packets are forwarded from the destination gateway application to the destination address in the *first protocol*" (emphasis added). This clearly contradicts the feature of claim 25 of "securing said *server* with a *second* security protocol" (emphasis added), because the server 18 of Gelman would use the *same* protocol (TCP/IP) as the client 10. Furthermore, there is no teaching of two different protocols each including an

encryption. Thus, Gelman not only does not teach the elements of claim 25 for which it was cited, but Gelman clearly teaches away from the claimed features.

Furthermore, the Examiner cites col. 3 lines 1-5, as teaching a "second security protocol". No such teaching exists. The cited section merely states that packets may be scrambled during transmission, and will thus need to be re-assembled in the proper order. This is not a "security protocol" but merely a symptom of the packetized data transmission, regardless of the protocol used. Thus, the section does not teach that for which it was cited.

Finally, the Examiner cites col. 31, lines 50-65 and col. 7, lines 15-30, as teaching a server "conversion" between a first protocol and a second protocol. However, the cited sections are discussing a conversion in the modified gateways 12, 16, not in a server (or not even in the users 10, 18). Thus, the reference does *not* teach the cited limitation that it is the server that performs the protocol conversion.

RFC2246 fails to overcome any of these cited shortcomings of Gelman, and thus for any of these reasons, claim 25 is patentable over the combination of references.

Claims 1-24 and 26-35 were rejected under 35 U.S.C. §103(a) as being unpatentable over Lincke *et al.* (U.S. 6,253,326) in view of "Wireless Authentication Protocol Wireless Transport Layer Specification" (WAP-WTLS). For the following reasons, the rejection is respectfully traversed.

Claim 1 recites a method for a terminal sending requests to a server via a gateway including the step of "converting between WTLS and said one or both of the SSL or the TLS security protocol in a secured domain of said server administrated by an administrator" wherein "WTLS encrypted packets sent by said terminal are routed by said gateway to said secured domain *without said gateway decrypting all of the encrypted packets* transported during a session" (emphasis added).

However, as previously argued, Lincke does not suggest the use of WTLS encrypted packets. Furthermore, as also previously discussed, the previous Examiner cited col. 111, lines 15-25 as teaching converting between WTLS to SSL

and/or TLS security protocols, but a reading of the cited passages does not support such a teaching. Instead, the passage merely discusses support for SSL and S-HTTP protocols, without any teaching of converting from WTLS to one of the supported protocols. Applicant could find no discussion anywhere in the reference for converting from one security protocol to another security protocol, each with an encryption.

The Examiner has failed to adequately address these previously supplied arguments. The reference Lincke does not teach packets being routed "by said gateway to said secured domain *without said gateway decrypting all of the encrypted packets* transported during a session".

The examiner states that Lincke reference teaches such a feature at various locations (see col.17, lines 40-50 and col. 113, line 15, cited on page 5 of the Office Action regarding rejection of claim 1; col. 18, lines 1-65, col. 83, lines 1-20, col. 92, lines 10-15, cited on page 10, of the Office action against claim 19; and col. 91, lines 50-60, cited on page 12, of the Office action against claims 26 and 31), but a close reading of these cited sections fails to support the Examiner's rejection.

Instead, Lincke deals with a *proxy* server, acting as a gateway between a wireless client and a content server on the Internet. One skilled in the art would know that the proxy server of the reference receives encrypted requests on the wireless side, **_decrypts them_**, reshapes them as internet requests, possibly as SSL secured requests, and transmits them to the content server on the Internet. It appears to be the aim of Lincke to encrypt only the traffic between the wireless client and the gateway, but not to the WEB server.

Within this embodiment, Lincke explicitly states that "the proxy server **_decrypts_** data before using SSL to transfer it to the context server, the unencrypted content resides in the proxy server memory for short periods of time" (see col. 91, l. 51-56; emphasis added) which clearly contradicts the statement of the Examiner on p. 12 of the new Office Action.

The system of Lincke differs then from of the present invention, because the encrypted requests are **_entirely decrypted_** in the gateway between the wireless

network and the Internet. The claims, however, specifically recite that the gateway **_does not decrypt the entire content of the requests_**. Only that information which is needed for *routing* the packets to their final destination would need be decrypted in the disclosed invention, not the entire contents. Thus, the decrypted data as disclosed in Lincke need not exist in the gateway of the claimed invention, and in fact, decrypting all of such contents is *prohibited* by the claim language. Accordingly, Lincke not only does not teach that for which it is cited, but it clearly teaches away from the cited claim language.

The Examiner repeatedly tries to use the Lincke tunneler 430 (Fig. 4) as the gateway of the claims, and the Lincke proxy server 180 (Fig. 4) as the secured domain of the claims; however, Lincke states that it is the proxy server 410 that is used as the gateway for the Internet (see col. 19, lines 39-51), and Lincke further states that the *proxy server* is required to accept, process, and reply to these tunneled packets (see col. 113, lines 61-64; see also col. 17, lines 42-46 and Fig. 5: tunneler 430 —> proxy server 180). The other citations of the Examiner do not reveal any additional embodiment that teaches the claimed material, and thus the reference does not teach that for which it was cited.

As clearly shown in Fig. 1 of Lincke, only the proxy server 180 could arguably act in some fashion as the gateway according to claim 1, because only the proxy server 180 arguably routes the packets to the internet, and the secured domain is a WEB or WAP server and is located entirely in the Internet, but such an interpretation would clearly make the claims patentable over the reference, because the proxy server 180 does not have all of the functionality of the gateway as defined in the claims.

Furthermore, Lincke does not disclose a WTLS-based gateway. Instead, the reference provides that the communication between the wireless user and the gateway is based on a proprietary CTP protocol encrypted according to a specific encryption scheme. Furthermore, Lincke does not disclose a WAP-enabled terminal, but rather a device and system of navigation of html-pages based on a special wireless protocol.

Furthermore, Lincke does not teach the step of claim 1 of "converting between WTLS and said one or both of the SSL or TLS security protocol in a secured domain of said server...", because the proxy server 180 already uses the SSL protocol (as cited by the Examiner in col. 91, lines 50-65). Thus there would be no functionality provided for a conversion with the WEB or WAB-server 140 from WTLS to SSL as claimed, and there is no suggestion to do so within Lincke, and further doing so would change the principle of operation of the server.

The WAP-WTLS reference provided by the Examiner fails to overcome the cited shortcomings of Lincke, and thus claim 1 is patentable over the references for at least the above reasons. Claims 2-18, which depend, directly or indirectly, on claim 1, are thus patentable over the reference for at least the same reasons.

Claim 19 recites similar limitations to claim 1, reciting a gateway including "means for transmitting said SSL-encrypted requests to a receiving server, wherein said gateway can recognize WTLS-encrypted packets that are to be sent on transparently and can convert said WTLS-encrypted packets into said SSL-encrypted request without decrypting the information contained in said WTLS-encrypted packets". Thus, claim 19 is patentable over the reference for at least some of the same reasons as claim 1. Furthermore, claim 19 recites that it is the *gateway* that performs the conversion. The Examiner has cited no gateway capable of performing the listed conversion in any of the references. Thus, claim 19 is patentable over the reference for this reason as well.

Furthermore, claim 19 recites the feature of "...wherein the gateway can recognize WTLS-encrypted packets that are to be sent on transparently and can convert said WTLS-encrypted packets into said SSL-encrypted request without decrypting the information contained in said WTLS-encrypted packets", which cannot be found in the proxy server 180, as previously pointed out. Claims 26 and 31 also recited similar features. Thus, these claims are patentable over the references for this reason as well.

Furthermore, as previously argued, claim 26 recites a request path of a "terminal generating a request including request packets encrypted using a WTLS protocol" through a gateway for "forwarding said request to said server or to another

server, wherein said gateway does not decrypt all of said request packets" to a server "decrypting some number of said request packets using said WTLS protocol". Claim 26 also recites a data path of said server or another server "serving data to said terminal via said gateway" also using the WTLS protocol, wherein "said gateway does not decrypt all of said data packets".

As discussed above, in previous responses, and at the previous personal interview, there is no suggestion in Lincke of using the WTLS protocol. Thus, claim 26 is patentable over the reference for this reason. Further, there is no suggestion of transmitting requests or data through a gateway *without decrypting* all of the WTLS encrypted packets (as discussed above for claim 1). Thus, for this reason as well, claim 26 is patentable over the reference.

Claims 20-24, which depend, directly or indirectly, on claim 19, are thus patentable over Lincke for at least the same reasons as claim 19.

Claims 27-30, which depend, directly or indirectly, on claim 26, are thus patentable over the reference for at least the same reasons as claim 26.

Claim 31 further recites a server and gateway similar to that in claim 26, using a WTLS encryption, wherein the gateway forwards said data to said terminal "without decrypting all of said data packets". Thus, claim 31 is patentable over the reference for similar reasons as claim 26. Claims 32-35, which depend, directly or indirectly, on claim 31, are thus patentable over the reference for at least the same reasons as claim 31.

New claims 36 and 37, which depend, respectively, on claims 1 and 19, are patentable for at least the same reasons as the parent claims. Furthermore, these claims recite that "said gateway determines whether an end-to-end secured routing is requested according to the URL of the requested page", which is a feature not found in any of the cited references, and thus they are patentable over the art of record for that reason as well.

In consideration of the foregoing analysis, it is respectfully submitted that the present application is in a condition for allowance and notice to that effect is hereby requested. If it is determined that the application is not in a condition for allowance,
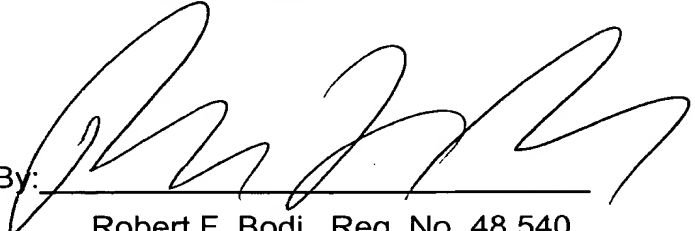
the examiner is invited to initiate a telephone interview with the undersigned attorney to expedite prosecution of the present application.

If there are any additional fees resulting from this communication, please charge same to our Deposit Account No. 16-0820, our Order No. 33544US1.

Respectfully submitted,

PEARNE & GORDON, LLP

By: _____

Robert F. Bodi, Reg. No. 48,540

1801 East 9th Street, Suite 1200
Cleveland, Ohio 44114-3108
(216) 579-1700

April 11, 2006